WEOS-17-01: Security Advisory

CRITICAL / **HIGH** / MEDIUM / LOW 2017-05-30

Description

This advisory contains information on how to mitigate a vulnerability reported in CVE-2016-10229 that affect **Viper12A** based products when the DHCP server is enabled (disabled by default).

A flaw in the Linux kernel version deployed with WeOS version 4.20 for Viper12A based products, when DHCP server is enabled, allow attackers with network access to a vulnerable WeOS to full root shell access.

The official CVE description of this vulnerability reads as follows:

CVE-2016-10229: udp.c in the Linux kernel before 4.5 allows remote attackers to execute arbitrary code via UDP traffic that triggers an unsafe second checksum calculation during execution of a recv system call with the MSG_PEEK flag.

Affected products

- The entire Viper 12A product line:
  - Viper-112A (all variants)
  - Viper-212A (all variants)

Impact

Successful exploitation of this vulnerability leads to full device compromise, granting an unauthorized attacker full access.

Our investigations have only found one execution path to this vulnerability. Following standard recommendations on network hardening, the risk is greatly reduced as the vulnerable DHCP service is disabled by default and typically only exposed to more secure networks when enabled.

Please consider our recommended mitigation below to minimize risk.

Severity

Our severity score is calculated as if the device where configured according to our recommendations.

The NVD CVSSv3 severity base score for this vulnerability is 9.8

The Westermo CVSSv3 severity base score for this vulnerability is **8.1**

Westermo Teleindustri AB
SE-640 40 Stora Sundby, Sweden
Tel. +46 (0)16 42 80 00 I Fax. +46 (0)16 42 80 01
info@westermo.com I www.westermo.com

Corp ID No: 556361-2604
VAT: SE556361260401

Mitigation

Only Viper12A based devices with WeOS version 4.20 and with the DHCP server enabled are affected.

With respect to deployment specific circumstances, users are advised to ensure the DHCP server is only exposed to internal (local) networks assuming they are considered more secure (or trusted).

Until the issue has been resolved and a fix is available, all devices that expose the DHCP server to external (less secure or less trusted) networks should consider either disabling the service and implemented static addresses, or implement port authentication 802.1x (also called NAP, network access protection or NAC, network access control).

Updates

A fix is in development and will be published at our web site as soon as it is generally available.

References

https://nvd.nist.gov/vuln/detail/CVE-2016-10229#vulnDescriptionTitle

Westermo Teleindustri AB
SE-640 40 Stora Sundby, Sweden
Tel. +46 (0)16 42 80 00 I Fax. +46 (0)16 42 80 01
info@westermo.com I www.westermo.com

Corp ID No: 556361-2604
VAT: SE556361260401